04-17-00

IBM Docket No. RSW9-2000-0038-US1

In the United States Patent and Trademark Office
Patent Application Transmittal

Transmitted herewith for filing is the Patent Application of:

Inventors(s): Mohammad Peyravian and Nevenko Zunic

For: Method and Apparatus for Secure Password Transmission and Password Changes

Enclosed are

16 pages of specification, including ***12*** claims, plus ***3*** sheets of ***formal*** drawings.

X An assignment of the invention to International Business Machines Corporation, Armonk, New York 10504.

A certified copy of a/an application.

X Declaration and Power of Attorney.

PTO-1449 & references

X A return post card

Other:

Filing Fee Calculation (For Other Than Small Entity)

Basic Fee:						$690.00
Claims Fees:	Filed	Limit	Extra		Rate per Extra	
Total claims:	12	20	0		$18.00	$0.00
Independent claims:	6	3	3		$78.00	$234.00
1	Multiple Dependent Claim Presented				$260.00	$260.00
					Total	**$1,184.00**

Please charge Deposit Account **09-0461** for the **Total** set forth above. The Commissioner is authorized to charge payment of any additional filing fees required under 37 CFR §1.16 and any patent application processing fees under 37 CFR §1.17 or to credit any overpayment to the identified account. A duplicate copy of this sheet is enclosed.

Express Mail Certificate

Express Mail Label No: EI922406413US

Date: April 14, 2000

I hereby certify that I am depositing the papers identified above with the U.S. Postal Service "Express Mail Post Office to Address" service on the above date, addressed to the Commissioner of Patents and Trademarks, Washington, DC 20231

Dianne Lane

Dianne Lane

BY: Jeanine S. Ray-Yarletts

Jeanine S. Ray-Yarletts

Attorney of Record Reg. No. 39,808

Date: April 14, 2000

IBM Corporation T81/062
Intellectual Property Law
PO Box 12195
Res. Tri. Park, NC 27709

Telephone: 919-543-2541 FAX 919-254-4330

EXPRESS MAIL LABEL NO.: EJ922406413US DATE OF DEPOSIT: April 14, 2000

I hereby certify that this paper and fee are being deposited with the United States Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to the Assistant Commissioner of Patents, Washington, D.C. 20231.

Dianne Lane
NAME OF PERSON MAILING PAPER AND FEE

Dianne Lane
SIGNATURE OF PERSON MAILING PAPER AND FEE

INVENTORS: Mohammad Peyravian and Nevenko Zunic

Method and Apparatus for Secure Password Transmission and Password Changes

Background of the Invention

In a networking environment, it is often the case that users interact with local application programs. The local application programs may exchange data with remote application programs on behalf of the users. When the remote application program controls resources of value, it most likely will require a user name (or userid) and password for verification and access control. Userids are considered, in most cases, to be public information, but passwords are considered to be private or secret. The local application program sends the userid and password combination to the remote application program over a network.

It is also very common for a server in a network of resources to be used to provide controlled access to the network or to applications residing within the network. Accordingly a server manages the resources and data for which it is responsible and facilitates access to the resources and data by networked machines which logged onto the network by way of credentials.

It is also common in the art for one or more network servers to be responsible for administering and limiting network access to clients for which valid account credentials have been provided during a network logon procedure. In this respect, the network server maintains a security database including account identification corresponding to users and services authorized to access the network and the protected network resources for which the network server enforces limited access.

It is sometimes necessary for the user to change his password to a new password. When the user wants to change the password, he submits his userid, old password and a new password to the local application program. The local application program then sends the userid, old password and new password combination to the remote application program over the network. When the network is not secure or is untrusted, the users' presumably secret passwords are susceptible to exposure and monitoring by unauthorized parties if the information is sent in the clear (i.e.. not encrypted or protected in some other manner). These outside parties could then replay the new password at some time in the future and gain access to the "protected" resources. To protect the passwords while traveling over public networks, some systems encrypt the passwords with symmetric-key crypto-systems (such as DES,RC5, etc.) or public-key cryptosystems (such as RSA, Elliptic curve, etc.). Encrypting the passwords in this way imposes additional overhead on the local and remote application programs. In addition to having to implement symmetric-key and/or public key crypto systems, they have to have either pre-established shared secret keys or to have a public-key infrastructure in place.

In the art of password security for logging onto a network, various distinct one-way hash functions are used on passwords to protect the secrecy of the passwords when they are transmitted on a non-secure network or transmission medium. Hash functions take an input string (the password) and convert it into an output string from which the input string cannot be determined (at least from a practical perspective the input string cannot be determined). These one-way hash functions are well suited for applications in which the receiving party does not need to know the input string corresponding to an output string in a received message. In this instance, when the user logs on to a network, the user's password is not sent across the network, only the hash of their password is sent, but this has not proven effective for the changing of passwords to the present time.

Encryption schemes have been incorporated into password change protocols to enable secure changing of a password stored at a remote computer. Under such schemes, the sender and receiver of the encrypted password change messages respectively know the operative encryption and decryption schemes. The sender encrypts the messages by applying an encryption scheme utilizing a key to the messages to be sent. The receiver decrypts the messages using a corresponding decryption scheme and corresponding key known by the receiver.

A method of changing passwords by a client was also described by Microsoft Corporation in their patent U.S. Patent number 5,719,941 filed January 12, 1996. In that patent, Microsoft describes a method of changing passwords wherein the client computes a first message (M1) by encrypting at least a new clear text password using a one-way hash function of the old password as the encryption key. A second message (M2) is computed by the client by encrypting at least the one-way hash of the old password with a one-way hash of the new password (as the encryption key). The client then transmits the first and second messages (M1 and M2) to the server. After receiving the first message, the server computes a decrypted first message, including at least the new clear text password by decrypting the received first message using a copy

of the one-way hash of the old password previously stored by the server as the decryption key. In this way, the new clear text password is obtained. While initially this seems to be an effective means of password changing, it is still open for replay or delay attacks by the unwanted intermediary. The intermediary could intercept the transaction and replay it at a later date.

The present invention presents a method for changing the password to a new password without requiring the use of a symmetric-key or public-key cryptosystem. It does not require a pre-established shared secret key or a public-key infrastructure. It only requires a collision-resistant hash function such as SHA-1 and ensures freshness (hence guarding against intercept and replay attacks) by incorporating random challenges.

Summary of the Invention

The present invention presents a secure method for changing a password to a new password when the passwords are being transmitted over untrusted networks. The present invention does not require the use of any additional keys (such as symmetric keys or public/private key pairs) to protect the password exchanges. Moreover, the present solution does not require the use of any encryption algorithms (such as DES, RC4/RC5, etc.). The present invention only requires the use of a collision-resistant hash function.

Brief Description of the Drawings

Figure 1 is a graphical representation of the minimal configuration on which the present invention will work.

Figure 2 is an information flow diagram of the password verification mechanism depicted in the preferred embodiment of the present invention.

Figure 3 is an information flow diagram of the password changing mechanism depicted in the present invention.

Objects of the Invention

It is an object of the invention to provide a secure means for a local computer user to change a password residing on a host computer without the need to have a public/private key pair or an agreed-upon symmetric key.

It is a further object of the invention to prevent these changed passwords from being intercepted and replayed by using nonces.

It is a further object of the invention to prevent predators from learning the passwords by not sending the new password across the network, and only sending a randomized digest of the password.

These and other objects of the invention will be presented with respect to the detailed description of the preferred embodiment.

Detailed Description of the Preferred Embodiment

The preferred embodiment presented is not meant to limit or restrict the invention in any way. It is meant to teach the skilled practitioner a method of performing the present invention. It will be clear to one skilled in the art that minor modifications to this preferred embodiment can be made without changing the described invention.

A view of the minimum configuration for an embodiment of the present invention is shown in Figure 1. Figure 1 depicts a system which has, at a minimum a local user machine **101**, or client machine and a host computer **103** or server machine. The local

computer and the host computer are connected together by way of a communications medium **105**. The communications medium could be, for example, telephone lines, digital satellite or radio communication. Any method of carrying computer communications is acceptable.

In the preferred embodiment, the password protection scheme used for this example will first be discussed. For convenience and ease for the reader, the local application program acting on behalf of the user will be referred to as the "client" and the remote application program to which the client is communicating will be referred to as the "server". For access to the resources at the remote host where the server programs reside, it is assumed that the user has a user identifier (userid) and a password (pw). Access to the server is controlled by a combination of the userid and pw. The password is considered to be a secret value that only the user and the server know. An alternative case would be that the secret password is known only to the user and the server knows a digest or hashed value of the password that it uses for verification. The userid is known to both the user and the server, but unlike the password, it is not meant to be a secret value. In the password mechanism described in the preferred embodiment of the present invention, the logon process occurs as follows:

First the user submits the userid and password to the client. The client then generates a random value (rc) and sends the userid and rc to the server. The server then generates a random value (rs) and sends it back to the client. The random values are called nonces or challenges The client generates a digest of the userid and password such that the digest is a hash function of the userid and password. There are many hash functions that can be used. It is suggested that a strong collision-resistant one-way hash function such as SHA-1 be used. Next the client generates a one-time authentication token such that the authentication token is a hash function of the digest, rc and rs. The authentication token is a one-time value since its value changes for each session due to the random values rc and rs. The inclusion of rc and rs help to

ensure the freshness of the communication. Because of the one-way hash function used, the authentication token does not reveal any information about the secret values (i.e.. the password or the digest). The client then sends the userid and the authentication token to the server. The server verifies the validity of the received authentication token and if it is valid, the user is allowed to access information residing at the server. This is more easily understood while referring to figure 2.

Figure 2 depicts the communications between the client and the server with respect to the password exchange. The client **201** first sends the userid and a random number (nonce - rc) **205** to the server **203**. The server **203** then sends a random number (nonce - rs) **207** to the client **201**. The client **201** responds to the server **203** by sending the userid and an authentication token where the authentication token is a hash of an idpw_digest, rc and rs and the idpw_digest is a hash of the userid and the password. The server then checks the validity of the authentication token using the servers copies of the idpw_digest, rc and rs. In this way the server can securely authenticate the user without having to actually know the password itself.

If for some reason the user wants to change their password, because the password has been discovered by someone else or because of the time-out mechanisms put in place to maintain secrecy of passwords, a method needs to be present to securely change the password so that no one other than the user/client and the intended server application discover the new password. In the preferred embodiment of the present invention, this is accomplished by using multiple hash algorithms on the userid, old and new passwords and random challenges or nonces sent between the client and the server.

With reference to Figure 3, the flow of information in the preferred embodiment will now be addressed. The user first submits their userid, existing password and new password to the client **301**. The client **301** generates a random value or nonce (rc) and sends the userid and the random value (rc) **305** to the server **303**. The server **303**

generates a random value or nonce (rs) and sends **307** it to the client. These random values are sometimes referred to as challenges. The client **301** generates a userid and password digest in addition to a userid and new password digest where the digest is calculated by performing a hash function on the userid and the respective password. It is recommended that a strong, collision-resistant one-way hash function such as SHA-1 be used. The client **301** then generates a one-time authentication token and a one-time authentication token mask value where the one-time authentication token is a hash function of the old userid-password digest, rc and rs and the authentication token mask is a hash function of the userid-password digest, rc plus some predetermined value and rs. The authentication token and the authentication token mask are one-time values since their values change in each session due to the random values rc and rs. Note that because of the one-way hash function, the authentication token and the authentication token mask do not reveal any information about the secret values of the password or the userid-password digest.

The client **301** next generates a value that we will call a protected_idpw_digest by exclusive-or'ing the hash of the userid and the new password and the authentication token mask. The client **301** then sends **309** the userid, authentication token and protected_idpw_digest to the server **303**. The server **303** verifies the validity of the received authentication token. If the authentication token is valid, the server **303** sends a message to the client accepting the password change **311**. If the authentication token is not valid, the password change is rejected **311**.

When the server verifies the authentication token values, the server must use its own copies of the userid-password digest, rc and rs. Using those values, the server must execute the hash function on them and compare the results with the authentication token received from the client. To retrieve the digest of the userid with the new password, the server generates the authentication token mask (as depicted above) and exclusively-or's it with the received protected_idpw_digest. Using this

mechanism, the server never stores the new password itself, it only stores the calculated digest of the userid and the new password.

What is claimed is:

1 - A computer network comprising:

a local computer;

a userid associated with a user of the local computer, said userid having a secret password associated therewith;

a host computer;

a communications mechanism connecting the host computer to the local computer wherein the local computer requests access to the host computer by:

sending the userid and a first nonce to the host computer;

the host computer responds to the local computer by sending a second nonce to the local computer;

the local computer then sends the host computer an authentication token comprising a hashed value of the combination of the userid and password, the first nonce and the second nonce;

the server verifies the hashed value using copies of the authentication token, first nonce and second nonce residing at the host computer;

the host computer allows the user at the local computer to access information at the host computer only if the verification is successful.

2- A computer network comprising:

a local computer;

a userid associated with a user of the local computer; said userid having an original password associated therewith;

a host computer; and,

a communications mechanism connecting the host computer to the local computer wherein the local computer accesses the host computer by using the original password and wherein the local computer changes the original password for accessing the host computer to a new password by sending a first random value and the userid of the user to the host computer, the host computer generates a second random value

and sends it to the local computer, the local computer generates an authentication token using a hash function, the userid, the original password and a digest of the new password and sends the authentication token and the digest to the host computer, wherein the host computer accepts the change of the password to the new password if the host computer can verify the authentication token.

3 - A network as claimed in claim 2 wherein the host computer verifies the authentication token using a copy of the first random value, a copy of the second random value and a copy of the authentication token residing at the host computer.

4- A network as claimed in claim 2 wherein said hash function is a collision-resistant, one-way hash.

5 - A method for accessing information on a host computer by a local computer over a network, the local computer having a user and a user identifier (userid) associated therewith, the userid also having a password associated therewith, the method comprising the steps of:

sending, by the local computer, a message across the network to the host computer, the message comprising the userid of the user at the local computer and a first nonce;

replying, by the host computer to the local computer, by sending a reply across the network, the reply comprising a second nonce;

creating, by the local computer, a userid-password digest using a hash function on the userid and the password;

calculating, by the local computer, an authentication token, the authentication token comprising a hashed value of the userid-password digest, the first nonce and the second nonce;

transmitting, by the local computer to the host computer, the userid and the authentication token;

verifying, by the host computer, that the authentication token is valid for the userid, the host computer using copies of the first nonce, the second nonce and the userid-password digest stored at the host computer;

allowing the user at the local computer to access information at the host computer only if the verification step is successful.

6. A method for securely changing an existing password associated with a user identifier (userid) on a host computer to a new password, wherein said passwords enable a user associated with said userid at a local computer to access information on said host computer across a network; said method comprising the steps of:

sending, by the local computer, the userid and a first nonce to the host computer;

replying, by the host computer to the local computer, with a second nonce;

generating, by the local computer, a first digest of the userid and the existing password and a second digest of the userid and the new password;

creating, by the local computer, an authentication token and an authentication token mask wherein said authentication token si a hash function of the first digest, first nonce and second nonce, and said token mask is a hash function of the second digest, first nonce plus a predetermined value and the second nonce;

generating, by the local computer, a protected digest by exclusive-or'ing the second digest with the token mask;

sending, by the local computer to the host computer, the userid, authentication token and the protected digest;

verifying, by the host computer, the validity of the authentication token; and,

accepting the new password to replace the existing password if the authentication token is valid.

7. A method as claimed in claim 5 wherein said first and second digests are calculated by performing a hash function on the userids and respective passwords.

8. A method as claimed in claim 5 or 6 wherein said hash function is a collision-resistant, one-way hash.

9 - A computer program product for accessing information on a host computer by a local computer over a network, the local computer having a user and a user identifier (userid) associated therewith, the userid also having a password associated therewith, the method comprising:

computer readable programming means for sending, by the local computer, a message across the network to the host computer, the message comprising the userid of the user at the local computer and a first nonce;

computer readable programming means for replying, by the host computer to the local computer, by sending a reply across the network, the reply comprising a second nonce;

computer readable programming means for creating, by the local computer, a userid-password digest using a hash function on the userid and the password;

computer readable programming means for calculating, by the local computer, an authentication token, the authentication token comprising a hashed value of the userid-password digest, the first nonce and the second nonce;

computer readable programming means for transmitting, by the local computer to the host computer, the userid and the authentication token;

computer readable programming means for verifying, by the host computer, that the authentication token is valid for the userid, the host computer using copies of the first nonce, the second nonce and the userid-password digest stored at the host computer;

computer readable programmnig means for allowing the user at the local computer to access information at the host computer only if the verification step is successful.

10. A computer program product for securely changing an existing password associated with a user identifier (userid) on a host computer to a new password, wherein said passwords enable a user associated with said userid at a local computer to access information on said host computer across a network; said method comprising the steps of:

computer readable programming means for sending, by the local computer, the userid and a first nonce to the host computer;

computer readable programming means for replying, by the host computer to the local computer, with a second nonce;

computer readable programming means for generating, by the local computer, a first digest of the userid and the existing password and a second digest of the userid and the new password;

computer readable programming means for creating, by the local computer, an authentication token and an authentication token mask wherein said authentication token is a hash function of the first digest, first nonce and second nonce, and said token mask is a hash function of the second digest, first nonce plus a predetermined value and the second nonce;

computer readable programming means for generating, by the local computer, a protected digest by exclusive-or'ing the second digest with the token mask;

computer readable programming means for sending, by the local computer to the host computer, the userid, authentication token and the protected digest;

computer readable programming means for verifying, by the host computer, the validity of the authentication token; and,

computer readable programming means for accepting the new password to replace the existing password if the authentication token is valid.

11. A computer program product as claimed in claim 10 wherein said first and second digests are calculated by performing a hash function the userids and respective passwords.

12. A computer program product as claimed in claim 10 or 11 wherein said hash function is a collision-resistent, one-way hash.

Abstract

A secure method for changing a password to a new password when the passwords are being transmitted over a network is presented. The present invention does not require the use of any additional keys (such as symmetric keys or public/private key pairs) to protect the password exchanges. Moreover, the present solution does not require the use of any encryption algorithms (such as DES, RC4/RC5, etc.), it only requires the use of a collision-resistant hash function.

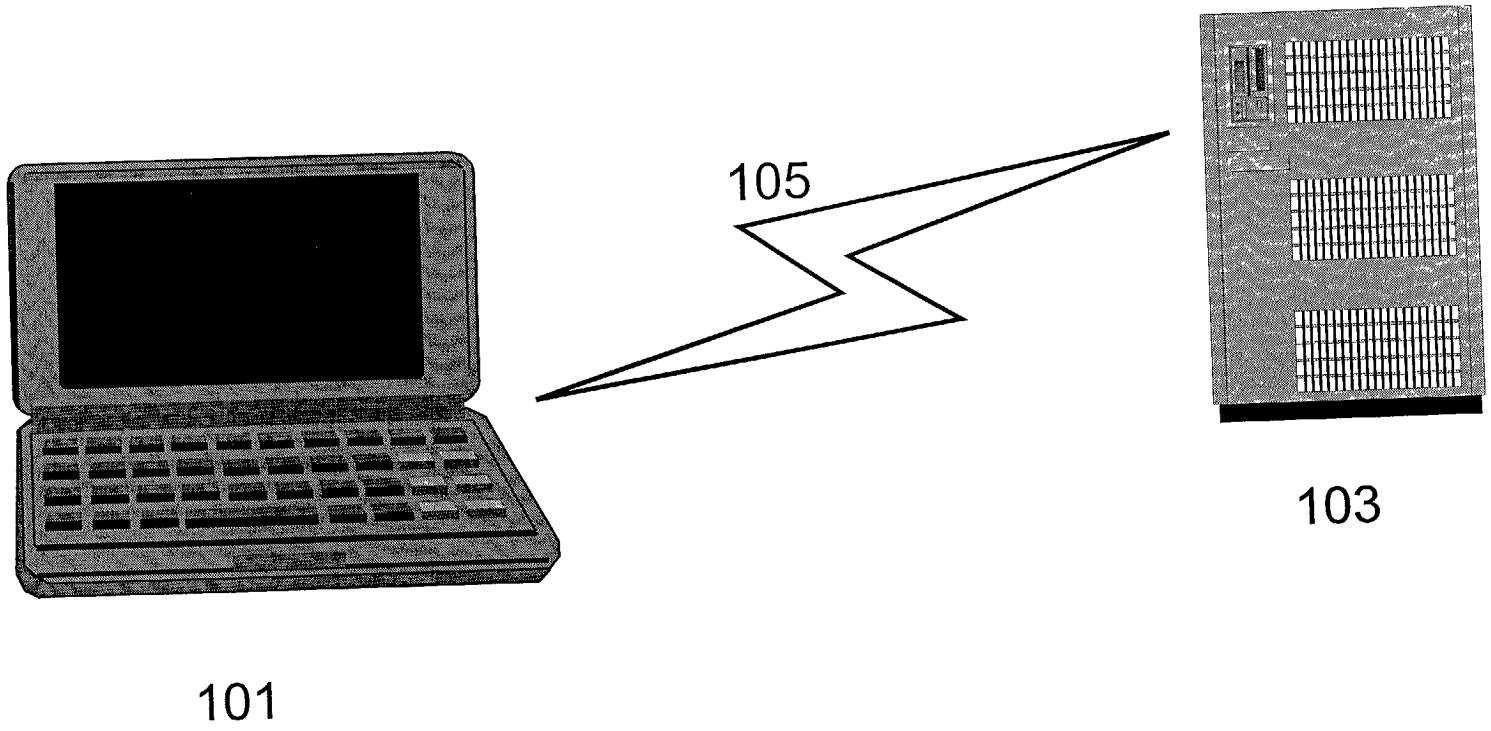

Fig. 1

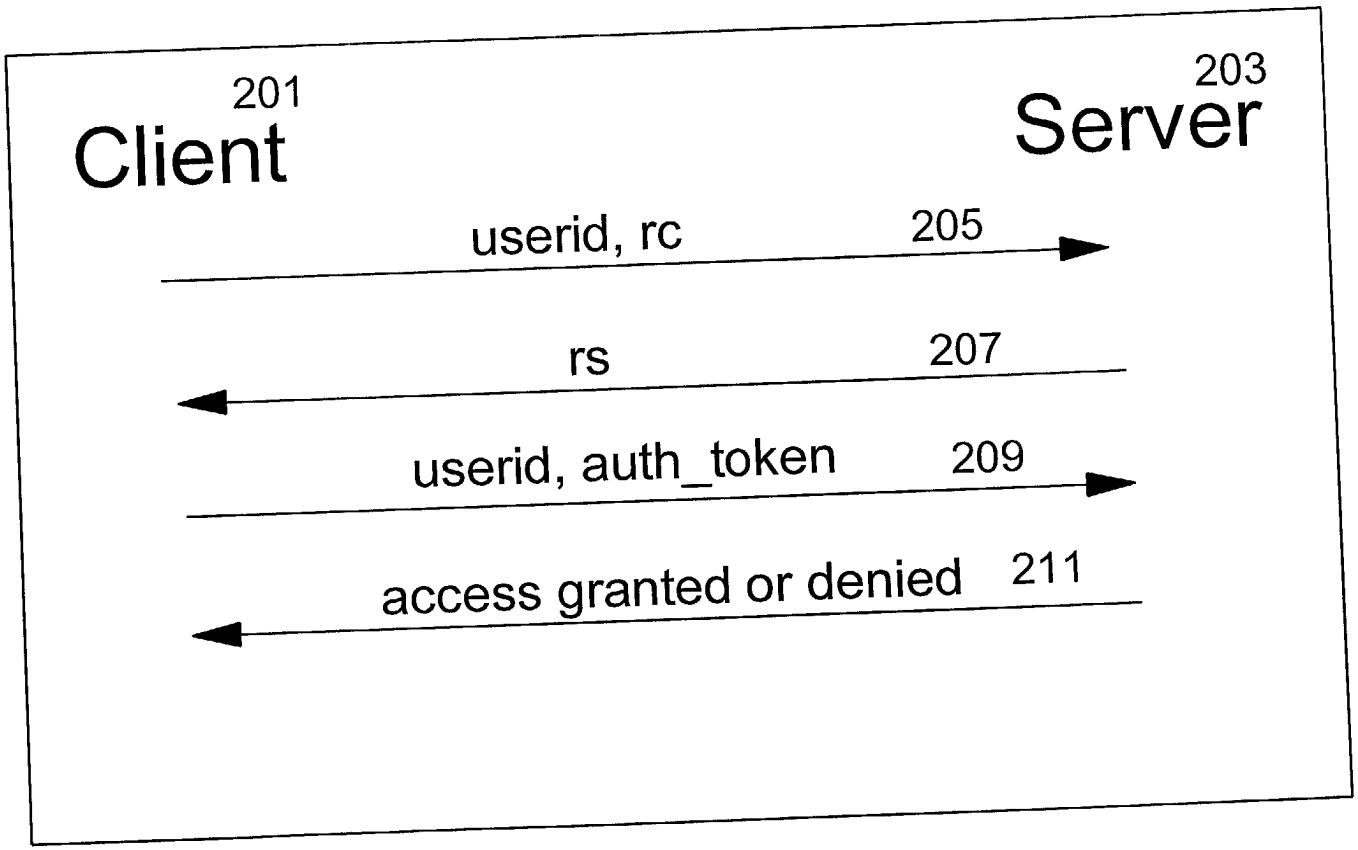
201
Client
203
Server
userid, rc
205
rs
207
userid, auth_token
209
access granted or denied
211

Fig. 2

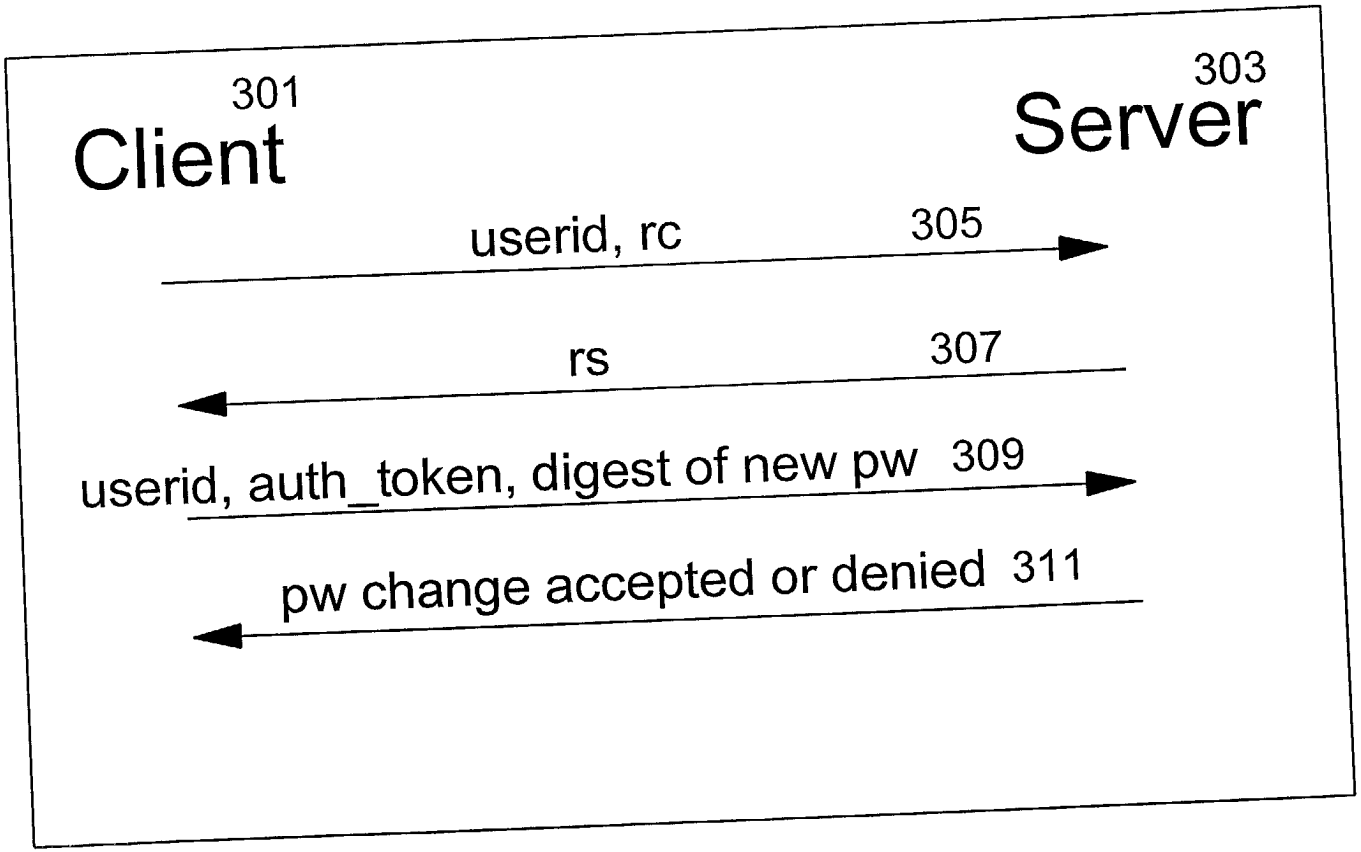
301
Client
303
Server
userid, rc
305
rs
307
userid, auth_token, digest of new pw
309
pw change accepted or denied
311

Fig. 3

IBM Docket No. RSW9-2000-0038-US1

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Method and Apparatus for Secure Password Transmission and Password Changes

the specification of which is identified by the attorney (IBM) Docket Number appearing above.

I hereby state that I have reviewed and understand the contents of the above- identified specification, including the claims

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Number	Country	Day/Month/Year	Priority Claimed

I hereby claim the benefit (a) under Title 35, United States Code, §119(e) of any U.S. application listed below and identified as a provisional application or (b) under Title 35, United States Code, §120 of any U.S. application listed below and not identified as a provisional application, and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior U.S. application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application

Prior U.S. Applications

Serial No.	Filing Date	Status

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

IBM Docket No. RSW9-2000-0038-US1

As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:
Bruce A. Clay, Reg. No. 32,121; Gregory M. Doudnikoff, Reg. No. 32,847; Edward H. Duffield, Reg. No. 25,970; Jerry W. Herndon, Reg. No. 27,901; Gerald R. Woods, Reg. No. 24,144; Jeanine S. Ray-Yarletts, Reg. No. 39,808; Joseph C. Redmond, Jr., Reg. No. 18,753; John E. Hoel, Reg. No. 26,279; Christopher A. Hughes, Reg. No. 26,914; and Edward A. Pennington, Reg. No. 32,588;

AND also

Send all correspondence to: Jeanine S. Ray-Yarletts, IBM Corporation T81/062; PO Box 12195; Research Triangle Park, NC 27709

First Inventor: Mohammad Peyravian

Signature: Mohammad Peyravian 4/13/00
Date

Residence: 122 Lake Hollow Circle, Cary, North Carolina 27513

Citizenship: United States of America

Post Office Address: same as residence

Second Inventor: Nevenko Zunic

Signature: Nevenko Zunic 4/10/2000
Date

Residence: 45 Reggie Drive, Wappingers Falls, New York 12590

Citizenship: United States of America

Post Office Address: same as residence